UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/763,732	02/27/2001	Wilhelmus Gerardus Petrus Mooij	82032-0005	9900

21186 7590 03/21/2007

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
COLIN, CARL G	
ART UNIT	PAPER NUMBER
2136	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	03/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	09/763,732	MOOIJ ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 December 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. In response to communications filed on 12/21/2006, the following claims 1-15 are presented for examination.

2. Applicant's arguments, filed on 12/21/2006, with respect to the rejection of claims 1-15 have been fully considered, but they are not persuasive. Applicant argues that Graunke et al does not disclose providing information on a protocol for communication between the content player and a secure device. Examiner respectfully disagrees. The "information on a protocol is provided as an interface or an applet" according to applicant's specification (page 4, lines 24-27); and Graunke et al discloses providing a key module as an interface or applet (plug-in) that meets the recitation of protocol information to the executable of trusted player (see column 7, lines 40-45), the key module is for communication between the trusted player (content player) and the storage medium (secure device) for accessing encrypted content in the storage medium, (see column 8, line 60 through column 9, line 2), the key module is arranged to transform encrypted symmetric keys (secure device data) into decrypted keys required to decrypt the encrypted data (see column 8, line 60 through column 9, line 2). Therefore, as explained above, Graunke et al discloses providing protocol information for communication between the content player and a secure device (for instance, column 4, lines 35-37 states, "the data on the storage medium (secure device) is accessed by a program such as storage device reader (player) via key module (interface)). Applicant generally alleges that since there is no teaching in Graunke et al

of providing information on a protocol for communication between the content player and a secure device, there is also no teaching in Graunke et al of attribute data comprises information to find in the protected content structure information on an appropriate protocol for establishing a communication interface between the content player and the secure device. Examiner respectfully disagrees. As shown above, Graunke et al discloses key module (interface) that allows the player to play encrypted content in the storage medium. As cited in the office action information is provided for checking the authenticity of the key module (i.e. ensuring it is an appropriate protocol) for establishing a communication interface between the content player and the secure device (see column 13, lines 47 through column 14, line 11 and column 9, line 55 through column 10, line 29). In addition, column 8, lines 10-31 shows an example of how the key module is built as to make it appropriate for the player and capable of verifying the player so that the player can be trusted to play the encrypted contents in the storage device. Therefore, applicant has not overcome the rejection in view of Graunke et al and the rejection is maintained.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-15 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 5,991,399 to **Graunke et al**.

As per claim 1, **Graunke et al** discloses a system for providing encrypted data in a content player comprising a decryption device comprising an encryption device for encrypting data using an encryption algorithm (see column 8, lines 1-5); a protection device for providing secure device data (keys) information on a protocol (key module) for communication between the content player and a secure device (storage medium) (see figure 1 and column 4, lines 33-51) arranged to transform the secure device data into information required to decrypt the encrypted data (see column 8, lines 1-8, lines 32-55, and lines 61-66); a control device for providing a protected contents structure containing encrypted data, secure device data, said protocol information and attribute data for finding relevant parts inside the protected contents structure (see column 8, lines 18-37 and column 13, line 47 through column 14, line 11); and wherein the attribute data comprises information to find in the protected contents structure information on an appropriate protocol for establishing a communication interface between the content player and the secure device for use of the secure device to transform secure device data communicated to the secure device through the communication interface into information required to decrypt the encrypted data (see column 7, lines 28-45 and column 13, line 47 through column 14, line 11; and column 9, line 55 through column 10, line 29).

As per claim 2, **Graunke et al** discloses wherein said protection device provides at least one secure device applet containing information on a protocol for communication (see column 7, lines 40-45 and column 8, lines 61-66).

As per claim 3, **Graunke et al** discloses a method for decrypting encrypted data in a content player comprising: an input for receiving protected contents containing encrypted data, secure device data, information on a protocol (key module) for communication between the content player and a secure device arranged to transform the secure device data into information required to decrypt the encrypted data and attribute data for finding relevant parts inside the protected contents (see figure 2 and column 6, lines 17-45), a decryption device (see column 14, line 4-8 and figure 5, element 214) and a control device (see column 13, lines 34-57), wherein said secure device data comprises information required to decrypt the encrypted data and wherein the attribute data comprises information to find in the protected contents information on an appropriate protocol for communication between the content player and a secure device (storage medium) (see figure 1 and column 4, lines 33-51) for retrieving the information required to decrypt the encrypted data (see column 13, line 47 through column 14, line 11); wherein the control device is programmed to use the attribute data to find the appropriate protocol information to establish a communication interface between the decryption device and a secure device used with the content player (see column 8, lines 18-31); wherein the decryption device is suitable for communicating with the secure device as controlled by the protocol information to obtain information required by the decryption device to decrypt the encrypted data and generated by the secure device by transforming secure device data communicated to the secure

device through the communication interface (see column 13, lines 47 through column 14, line 11 and column 9, line 55 through column 10, line 29).

As per claim 4, **Graunke et al** discloses wherein said information on the appropriate protocol for communication between the content player and the secure device is provided as a secure device applet wherein the control device is programmed to operate as a virtual machine to execute the secure device applet to establish said communication interface (see column 7, lines 33-45 and column 4, lines 33-51).

As per claim 5, **Graunke et al** discloses wherein at least one secure device applet in the protected contents is authenticated (see column 8, lines 46-49), wherein the control device comprises an applet loader for verifying the authentication of a secure device applet, wherein only a verified secure device applet is loaded into the virtual machine (see column 8, lines 24-32 and lines 46-49).

As per claim 6, **Graunke et al** discloses wherein at least one secure device applet in the protected contents is encrypted wherein the applet loader is suitable for decrypting an encrypted secure device applet (see column 8, lines 1-5 and lines 18-47).

As per claim 7, **Graunke et al** discloses wherein the virtual machine comprises a content player application program interface and a security application program interface, the secure

device applet communicating with the content player and the secure device by means of said interfaces (see column 6, lines 22-55).

As per claim 8, **Graunke et al** discloses the limitation of wherein the control device is arranged to determine of which type the secure device used in the system is, wherein the control device is arranged to retrieve a secure device applet from the protected contents corresponding with the type of secure device (see column 6, line 46 through column 7, line 15 and column 7, lines 29-45).

As per claim 9, **Graunke et al** discloses the limitation of wherein the system is part of a content player connected to a network, wherein the control device is arranged to determine the type of secure device used in the system, and wherein the control device is arranged to request a corresponding secure device applet to be downloaded from a service provider (see column 7, lines 4-45).

As per claim 10, **Graunke et al** discloses a method for providing communication interface between a decryption device and a secure device in a content player comprising: receiving a protected contents structure containing encrypted data, secure device data, information on a protocol (key module) for communication between the content player and a secure device (storage medium) (see figure 1 and column 4, lines 33-51) arranged to transform the secure device data into information required to decrypt the encrypted data and attribute data for finding relevant parts inside the protected contents structure (see column 6, lines 17-45 and

column 9, line 55 through column 10, line 29); wherein said secure device data comprises information required to decrypt the encrypted data and wherein the attribute data comprises information to find in the protected contents information on an appropriate protocol for communication between the content player and a secure device for retrieving the information required to decrypt the encrypted data (see column 13, line 47 through column 14, line 11 and column 7, lines 28-45); retrieving said protocol information from the protected contents structure to establish a communication interface between the decryption device and a secure device used with the content player (see column 8, lines 18-31 and column 9, line 55 through column 10, line 29) to transform secure device data communicated to the secure device through the communication interface into information required to decrypt the encrypted data (see column 13, lines 47 through column 14, line 11 and column 9, line 55 through column 10, line 29).

As per claim 11, **Graunke et al** discloses the limitation of wherein said protocol information is provided as a secure device applet, wherein the secure device applet is executed in a virtual machine to establish the communication interface (see column 7, lines 33-45 and column 4, lines 33-51).

As per claim 12, **Graunke et al** discloses the limitation of detecting which type of secure device is being used with the content player and requesting corresponding protocol information or a secure device applet from a source providing the protected contents structure (see column 6, line 46 through column 7, line 15 and column 7, lines 29-45).

As per claim 13, **Graunke et al** discloses the limitation of detecting which type of secure device is being used with the content player and requesting corresponding protocol information or a secure device applet from a source providing the protected contents structure (see column 6, line 46 through column 7, line 15 and column 7, lines 29-45).

As per claim 14, **Graunke et al** discloses wherein said protocol information or secure device applet is authenticated (see column 8, lines 46-49), further comprising verifying the authentication and using only verified protocol information or a verified secure device applet to establish said communication interface (see column 8, lines 24-32 and lines 46-49).

As per claim 15, **Graunke et al** discloses a method for broadcasting protected contents comprising: encrypting data using an encryption algorithm (see column 8, lines 1-5); providing secure device data, providing information on a protocol (key module) for establishing a communication interface between the content player and a secure device (storage medium) (see figure 1 and column 4, lines 33-51) arranged to transform the secure device data communicated to the secure device through the communication interface into information required to decrypt the encrypted data (see column 8, lines 1-8, lines 32-55, and lines 61-66); providing protected contents containing the encrypted data, the secure device data, the protocol information and attribute data (see column 8, lines 18-37 and column 13, line 47 through column 14, line 11); and broadcasting the protected contents (see column 3, lines 61-67); wherein the attribute data comprises information to find in the protected contents structure information on an appropriate protocol for communication between the content player and the secure device (see column 7,

lines 28-45 and column 13, line 47 through column 14, line 11; and column 9, line 55 through column 10, line 29).

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

4.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cc

Carl Colin
Patent Examiner
March 15, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

3/15/07